(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10269060 A**

(43) Date of publication of application: **09.10.98**

(51) Int. Cl **G06F 7/72**
G09C 1/00
// G06F 17/10

(21) Application number: **10014250**

(22) Date of filing: **27.01.98**

(30) Priority: **27.01.97 JP 09 12667**

(71) Applicant: **TOSHIBA CORP**

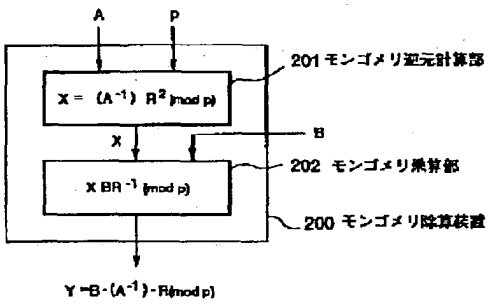
(72) Inventor: **SHINPO ATSUSHI**

(54) MONTGOMERY DIVISION DEVICE, MONTGOMERY INVERSE ELEMENT CALCULATION DEVICE, MONTGOMERY DIVISION METHOD AND MONTGOMERY INVERSE ELEMENT CALCULATION METHOD

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a Montgomery division device capable of obtaining a divided result in a Montgomery arithmetic area at a high speed.

SOLUTION: This Montgomery division device 200 for obtaining the divided result Y in the Montgomery arithmetic area to be Y=B.A' (-1).2 n mod N for the integer (n) of (n)≧L when a bit length at the time of binarily expressing N is defined as L for a positive integer N, the positive integer A (0≦A<N and A and N are mutually prime) and the positive integer B is provided with a Montgomery inverse element calculation part 201 for inputting the integer A and a modulus N and obtaining an inverse element X=A (-1).2 (2n) mod N and a Montgomery multiplication part 202 for inputting the obtained inverse element X, the modulus N and the B and obtaining the divided result Y=B.X.2 (-n) mod N.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－269060

(43)公開日　平成10年(1998)10月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　7/72		Ｇ０６Ｆ　7/72	
Ｇ０９Ｃ　1/00	６５０	Ｇ０９Ｃ　1/00	６５０Ａ
// Ｇ０６Ｆ　17/10		Ｇ０６Ｆ　15/31	Ｚ

審査請求　未請求　請求項の数12　ＯＬ　（全 18 頁）

(21)出願番号　特願平10－14250

(22)出願日　平成10年(1998)１月27日

(31)優先権主張番号　特願平9－12667

(32)優先日　平９(1997)１月27日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　新保　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

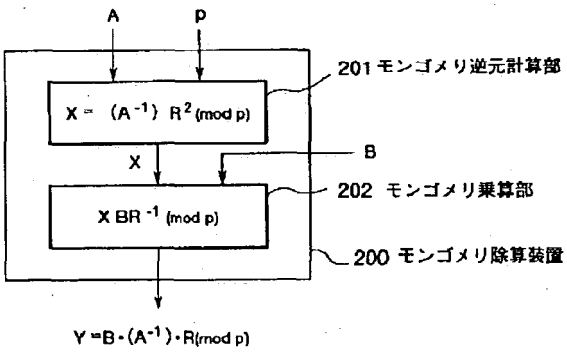
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　モンゴメリ除算装置及びモンゴメリ逆元計算装置並びにモンゴメリ除算方法及びモンゴメリ逆元計算方法

(57)【要約】

【課題】　本発明は、モンゴメリ演算域での除算結果を高速に求めることのできるモンゴメリ除算装置を提供すること。

【解決手段】　正の整数Ｎ、正の整数Ａ（０≦Ａ＜Ｎ、ＡとＮは互いに素）、正の整数Ｂについて、Ｎを２進表現したときのビット長をＬとして、ｎ≧Ｌなる整数ｎに対して、Ｙ＝Ｂ・Ａ＾（－１）・２＾ｎ　ｍｏｄ　Ｎなるモンゴメリ演算域での除算結果Ｙを求めるモンゴメリ除算装置であって、整数Ａと法Ｎを入力として逆元Ｘ＝Ａ＾（－１）・２＾（２ｎ）　ｍｏｄ　Ｎを求めるモンゴメリ逆元計算部と、求められた逆元Ｘと法ＮとＢを入力として除算結果Ｙ＝Ｂ・Ｘ・２＾（－ｎ）　ｍｏｄ　Ｎを求めるモンゴメリ乗算部とを備えたことを特徴とする。



1

【特許請求の範囲】

【請求項１】正の整数N、正の整数A（０≦A＜N、AとNは互いに素）、正の整数Bについて、Nを２進表現したときのビット長をLとして、n≧Lなる整数nに対して、$Y=B\cdot A^{-1}\cdot 2^{n} \mod N$なるモンゴメリ演算域での除算結果Yを求めるモンゴメリ除算装置であって、

整数Aと法Nを入力として逆元$X=A^{-1}\cdot 2^{2n} \mod N$を求めるモンゴメリ逆元計算手段と、

求められた逆元Xと法NとBを入力として除算結果$Y=B\cdot X\cdot 2^{-n} \mod N$を求めるモンゴメリ乗算手段とを備えたことを特徴とするモンゴメリ除算装置。

【請求項２】前記モンゴメリ逆元計算手段は、

整数Aと法Nを入力として中間結果$C=A^{-1}\cdot 2^{k} \mod N$とパラメータk（L≦k≦２L）を求める逆元計算手段と、

求められた中間結果Cとパラメータkと法Nを入力として逆元$X=C\cdot 2^{2n-k} \mod N$を求める逆元補正手段とを有することを特徴とする請求項１に記載のモンゴメリ除算装置。

【請求項３】正の整数N、正の整数A（０≦A＜N、AとNは互いに素）、正の整数Bについて、Nを２進表現したときのビット長をLとして、n≧Lなる整数nに対して、$Y=B\cdot A^{-1}\cdot 2^{n} \mod N$なるモンゴメリ演算域での除算結果Yを求めるモンゴメリ除算装置であって、

整数Aと法Nを入力として第１の中間結果$C=A^{-1}\cdot 2^{k} \mod N$とパラメータk（L≦k≦２L）を求める逆元計算手段と、

求められた第１の中間結果Cと法NとBを入力として第２の中間結果$D=B\cdot C\cdot 2^{-n} \mod N$を求めるモンゴメリ乗算手段と、

このモンゴメリ乗算手段により求められた第２の中間結果Dと前記逆元計算手段により求められたパラメータkと法Nを入力として除算結果$Y=D\cdot 2^{2n-k} \mod N$を求める逆元補正手段とを備えたことを特徴とするモンゴメリ除算装置。

【請求項４】正の奇整数N、正の整数A（０≦A＜N、AとNは互いに素）について、Nを２進表現したときのビット長をLとして、n≧Lなる整数nに対して、$X=A^{-1}\cdot 2^{2n} \mod N$なるモンゴメリ演算域での逆元Xを求めるモンゴメリ逆元計算装置であって、

整数Aと法Nを入力として中間結果$C=A^{-1}\cdot 2^{k} \mod N$とパラメータk（L≦k≦２L）を求める逆元計算手段と、

求められた中間結果Cとパラメータkと法Nを入力として逆元$X=C\cdot 2^{2n-k} \mod N$を求める逆元補正手段とを備えたことを特徴とするモンゴメリ逆元計算装置。

【請求項５】内部に中間変数を記憶する複数のレジスタと、

2

前記レジスタを右または左にシフトするビットシフト器と、

２つのレジスタの内容の加算または減算を行う加減算器と、

２つのレジスタの内容の大小比較およびレジスタ内部の所定のビット位置の値の判定を行う判定器とを用いて前記逆元計算部および前記逆元補正部を構成することを特徴とする請求項４に記載のモンゴメリ逆元計算装置。

【請求項６】正の奇整数N、正の整数A（０≦A＜N、AとNは互いに素）について、Nを２進表現したときのビット長をLとして、n≧Lなる整数nに対して、$X=A^{-1}\cdot 2^{2n} \mod N$なるモンゴメリ演算域での逆元Xを求めるモンゴメリ逆元計算装置であって、

初期状態を２進表現にてU＝N、V＝A、T＝０、S＝１、k＝０とし、

Uの最下位ビットが０ならば、Uを右シフトし、Sを左シフトし、kを１増加するとともに、Vの最下位ビットが０ならば、Vを右シフトし、Tを左シフトし、kを１増加する処理と、

Uの最下位ビットが１かつVの最下位ビットが１で、U＞Vならば、UからVを減じ、Uを右シフトし、TにSを加え、Sを左シフトし、kを１増加する処理と、

Uの最下位ビットが１かつVの最下位ビットが１で、U≦Vならば、VからUを減じ、Vを右シフトし、SにTを加え、Tを左シフトし、kを１増加する処理からなる一連のループ処理を、V＞０の間、繰り返し、

V＝０になった場合、T≧NならばTからNを減じた後に、NからTを減じた値をTとし、T＜NならばNからTを減じた値をTとする逆元計算手段と、

初期状態をi＝０とし、

前記逆元計算手段により求められたTを左シフトした後、T≧NならばTからNを減じてiを１増加し、T＜Nならばiを１増加するループ処理を、$i<2n-k$の間、繰り返し、

$i=2n-k$になったときのTを逆元Xとする逆元補正手段とを備えたことを特徴とするモンゴメリ逆元計算装置。

【請求項７】初期状態としてNが設定されるUレジスタと、

初期状態としてAが設定されるVレジスタと、

初期状態として０が設定されるTレジスタと、

初期状態として１が設定されるSレジスタと、

初期状態として０が設定されるkレジスタと、

Uレジスタの右シフト、Vレジスタの右シフト、Tレジスタの左シフト、およびSレジスタの左シフトのうち指定されたものを実行するビットシフト器と、

UレジスタからVレジスタの内容を減じる処理、VレジスタからUレジスタの内容を減じる処理、TレジスタにSレジスタの内容を加える処理、SレジスタにTレジスタの内容を加える処理、TレジスタからNを減じる処

理、Nからレジスタの内容を減じる処理、およびkレジスタに1を加える処理のうち指定されたものを実行する加減算器と、

Uレジスタの最下位ビットが0であるか否か、Vレジスタの最下位ビットが0であるか否か、Vレジスタの値が0になったか否か、およびTレジスタの値がN以上であるか否かを判断する判定器と、

前記ビットシフト器、前記加減算器および前記判定器を制御する制御部を備えたことを特徴とする請求項6に記載のモンゴメリ逆元計算装置。

【請求項8】正の整数N、正の整数A（$0 \leqq A < N$、AとNは互いに素）、正の整数Bについて、Nを2進表現したときのビット長をLとして、$n \geqq L$なる整数nに対して、$Y = B \cdot A^{-1} \cdot 2^n \mod N$なるモンゴメリ演算域での除算結果Yを求めるモンゴメリ除算方法であって、

整数Aと法Nを入力として逆元$X = A^{-1} \cdot 2^{2n} \mod N$を求める第1のステップと、

求められた逆元Xと法NとBを入力として除算結果$Y = B \cdot X \cdot 2^{-n} \mod N$を求める第2のステップとを有することを特徴とするモンゴメリ除算方法。

【請求項9】前記第1のステップは、

整数Aと法Nを入力として中間結果$C = A^{-1} \cdot 2^k \mod N$とパラメータk（$L \leqq k \leqq 2L$）を求め、

求められた中間結果Cとパラメータkと法Nを入力として逆元$X = C \cdot 2^{2n-k} \mod N$を求めるものであることを特徴とする請求項8に記載のモンゴメリ除算方法。

【請求項10】正の整数N、正の整数A（$0 \leqq A < N$、AとNは互いに素）、正の整数Bについて、Nを2進表現したときのビット長をLとして、$n \geqq L$なる整数nに対して、$Y = B \cdot A^{-1} \cdot 2^n \mod N$なるモンゴメリ演算域での除算結果Yを求めるモンゴメリ除算方法であって、

整数Aと法Nを入力として第1の中間結果$C = A^{-1} \cdot 2^k \mod N$とパラメータk（$L \leqq k \leqq 2L$）を求める第1のステップと、

この第1のステップにより求められた第1の中間結果Cと法NとBを入力として第2の中間結果$D = B \cdot C \cdot 2^{-n} \mod N$を求める第2のステップと、

この第2のステップにより求められた第2の中間結果Dと前記第1のステップにより求められたパラメータkと法Nを入力として除算結果$Y = D \cdot 2^{2n-k} \mod N$を求める第3のステップとを有することを特徴とするモンゴメリ除算方法。

【請求項11】正の奇整数N、正の整数A（$0 \leqq A < N$、AとNは互いに素）について、Nを2進表現したときのビット長をLとして、$n \geqq L$なる整数nに対して、$X = A^{-1} \cdot 2^{2n} \mod N$なるモンゴメリ演算域での逆元Xを求めるモンゴメリ逆元計算方法であって、

整数Aと法Nを入力として中間結果$C = A^{-1} \cdot 2^k \mod N$とパラメータk（$L \leqq k \leqq 2L$）を求め、

求められた中間結果Cとパラメータkと法Nを入力として逆元$X = C \cdot 2^{2n-k} \mod N$を求めることを特徴とするモンゴメリ逆元計算方法。

【請求項12】正の奇整数N、正の整数A（$0 \leqq A < N$、AとNは互いに素）について、Nを2進表現したときのビット長をLとして、$n \geqq L$なる整数nに対して、$X = A^{-1} \cdot 2^{2n} \mod N$なるモンゴメリ演算域での逆元Xを求めるモンゴメリ逆元計算方法であって、

初期状態を2進表現にて$U = N$、$V = A$、$T = 0$、$S = 1$、$k = 0$とし、

Uの最下位ビットが0ならば、Uを右シフトし、Sを左シフトし、kを1増加するとともに、Vの最下位ビットが0ならば、Vを右シフトし、Tを左シフトし、kを1増加する処理と、

Uの最下位ビットが1かつVの最下位ビットが1で、$U > V$ならば、UからVを減じ、Uを右シフトし、TにSを加え、Sを左シフトし、kを1増加する処理と、

Uの最下位ビットが1かつVの最下位ビットが1で、$U \leqq V$ならば、VからUを減じ、Vを右シフトし、SにTを加え、Tを左シフトし、kを1増加する処理からなる一連のループ処理を、$V > 0$の間、繰り返し、

$V = 0$になった場合、$T \geqq N$ならばTからNを減じた後に、NからTを減じた値をTとし、$T < N$ならばNからTを減じた値をTとする第1のステップと、

初期状態をi＝0とし、

前記第1のステップにより求められたTを左シフトした後、$T \geqq N$ならばTからNを減じてiを1増加し、$T < N$ならばiを1増加するループ処理を、$i < 2n - k$の間、繰り返し、

$i = 2n - k$になったときのTを逆元Xとする第2のステップとを有することを特徴とするモンゴメリ逆元計算方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、計算機ネットワークでのデータ通信におけるデータの暗号化や通信相手の確認に利用される公開鍵暗号など奇数の整数を法とする多倍長の四則演算を繰り返し利用する処理のためのモンゴメリ除算装置及びモンゴメリ逆元計算装置並びにモンゴメリ除算方法及びモンゴメリ逆元計算方法に関する。

【０００２】

【従来の技術】情報通信ネットワークや計算機システムでは、電子的な情報の交換・蓄積が行われる。そのようなシステムが、大規模化し不特定多数のユーザが利用する状況では、悪意のユーザによる情報の盗聴や改ざんなどが問題となり、その対策として公開鍵暗号技術を利用する場合が多い。

【０００３】公開鍵暗号では、多倍長の奇整数を法とする演算で実現される方式が多く、その高速化が性能に影

響を与える。多倍長の奇整数を法とする四則演算の中では、特に乗算と除算が処理時間に与える影響が大きい。このうち、乗算を繰り返し実行する場合に適した計算アルゴリズムとして、モンゴメリ算法が知られている。

モンゴメリ算法は文献（１）Ｐ．Ｌ．Ｍｏｎｔｇｏｍｅｒｙ、“Ｍｏｄｕｌａｒｍｕｌｔｉｐｌｉｃａｔｉｏｎ　ｗｉｔｈｏｕｔ　ｔｒｉａｌ　ｄｉｖｉｓｉｏｎ”、Ｍａｔｈ．　ｏｆ　Ｃｏｍｐ．、Ｖｏｌ．４４、Ｎｏ．１７０、ｐｐ．５１９－５２１（１９８５）に詳しい。

【０００４】モンゴメリ算法は多倍長の剰余乗算を多倍長乗算２回程度の処理量で計算する方法である。多倍長の剰余算は多倍長の乗算よりも性能が劣ることが多く、その分の高速化が実現できる。このモンゴメリ算法はモンゴメリ演算域の元（これも同じ剰余系である）の乗算アルゴリズムであり、一般の剰余系での乗算をするには、まず乗数と被乗数をモンゴメリ演算域に変換し、次にモンゴメリ乗算を行ない、最後にモンゴメリ演算域から元の剰余系に結果を逆変換する。モンゴメリ変換とモンゴメリ逆変換はいずれも多倍長乗算１回程度の処理であるため、剰余乗算を繰り返し行なう、べき乗演算では変換と逆変換のオーバーヘッドが少なく、高速化が可能である。したがって、ＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ）暗号など多くの公開鍵暗号では、剰余系でのベキ乗剰余演算$c=m^e \mod N$をその基本演算としているため、このモンゴメリ算法を有効に利用することができる（ただし、単純にいくつかの乗算を行なうだけの場合には、変換と逆変換のオーバーヘッドのため必ずしも効率化にはつながらない）。

【０００５】ところで、近年、新しい暗号方式が種々研究・提案されており、例えば楕円曲線暗号が公開鍵暗号の中で注目を集めている。これは、楕円曲線上の離散対数問題がＲＳＡ暗号のベースとなっている合成数の素因数分解に比べて計算量的に困難であるという予想に基づいている。

【０００６】ここで、楕円曲線暗号の基本演算について簡単に説明する。

【０００７】有限体Ｆｐ（ただし、ｐ＞３）において、

$E(a,b)/Fp: y^2=x^3+ax+b \mod p$

ただし、$0\leq a, b<p$なる整数、$4a^3+27b^2\neq 0 \mod p$で定義される曲線を有限体Ｆｐ上の楕円曲線という。楕円曲線上の点とは、上式を満たす（ｘ，ｙ）の組（ただし、$0\leq x, y<p$なる整数）に無限遠点Ｏを加えたものをいう。この無限遠点Ｏは加算に関する単位元となる。

【０００８】楕円曲線上の点は以下に示す加算に関して群をなす。楕円曲線上の点$P=(x_1, y_1)$、$Q=(x_2, y_2)$の加算点を$S(x_3, y_3)$とすると、次のようになる。ただし、$-P=(x_1, -y_1)$である。

【０００９】（１）Ｑが単位元Ｏのとき、

$S=P+Q=Q+P=P$

（２）$Q=-P$のとき、

$S=P+Q=Q+P=O$

（３）$P\neq Q$のとき（ただし上記（１）（２）以外）、

$x_3=(y_2-y_1)^2/(x_2-x_1)^2-x_1-x_2 \mod p$

$y_3=(y_2-y_1)(x_1-x_3)/(x_2-x_1)-y_1 \mod p$

（４）$P=Q$のとき、

・$y_1\neq 0$の場合

$x_3=(3x_1^2+a)^2/(2y_1)^2-2x_1 \mod p$

$y_3=(3x_1^2+a)(x_1-x_3)/(2y_1)-y_1 \mod p$

・$y_1=0$の場合

$S=O$

また、楕円曲線上の点$P=(x_1, y_1)$のｅ（整数）倍演算は上記加算の繰り返しとして次のように定義される。

$eP=P+P+\cdots+P$（Ｐをｅ回加算する）

ただし、$e<0$の場合は、点（－Ｐ）を（－ｅ）倍する（（－ｅ）は正である）。$e=0$のときには$0P=O$とする。

【００１０】楕円曲線暗号では、この楕円曲線上の点のスカラー倍演算（ベキ加算）が基本演算となる。例えば、楕円ＥｌＧａｍａｌ暗号、楕円ＥｌＧａｍａｌ署名、楕円ＤＨなどにおける処理の大半を占める演算である。

【００１１】したがって、ＲＳＡ暗号が剰余乗算を基本演算としているのに対して、楕円曲線暗号では、基本演算を実現するのに四則演算が必要となる。

【００１２】さて、楕円曲線暗号のように基本演算が多倍長の四則演算の繰り返し処理であるような場合、四則演算の中で処理に時間を要するものは、剰余乗算および剰余除算であり、暗号処理全体を高速化するには、これら剰余乗算および剰余除算を高速化する必要がある。このうち前者の剰余乗算は、文献（１）のモンゴメリ乗算のアルゴリズムなどを用いれば良い。

【００１３】一方、剰余除算は逆元計算と剰余乗算との組合せで実現でき、一般に逆元は拡張ユークリッド互除法と呼ばれる算法で計算できる。しかし、一般にこのアルゴリズムはそれほど高速ではない。より高速な逆元の計算法として、多倍長整数の右シフト（１／２倍）、加算、減算で構成された計算法が、例えば文献（２）Ｋａｌｉｓｋｉ、Ｂ．Ｓ、Ｊｒ．、“Ｔｈｅ　Ｍｏｎｔｇｏｍｅｒｙ　ｉｎｖｅｒｓ　ａｎｄ　ｉｔｓ　ａｐｐｌｉｃａｔｉｏｎ”、ＩＥＥＥ　Ｔｒ．　Ｃｏｍｐ．、Ｖｏｌ．４４、Ｎｏ．８、ｐｐ．１０６４－１０６５、（Ａｕｇ．１９９５）に示されている。

【００１４】しかしながら、前述の文献（１）のモンゴメリ乗算と文献（２）の剰余系での除算の高速計算法をそのまま適用することはできない。なぜなら、モンゴメリ演算域と元の剰余系との変換・逆変換を乗算や除算のたびに実行しなければならず、オーバーヘッドが大きくなるからである。

【００１５】また、剰余除算をモンゴメリ演算域で効率良く求めるアルゴリズムはなかった。

【００１６】このように、剰余除算を高速化することは困難であるという問題点があった。

【００１７】したがって、楕円曲線暗号のように基本演算が四則演算（剰余系演算）の繰り返し処理であるような暗号の処理を高速化することは困難であるという問題点があった。

【００１８】

【発明が解決しようとする課題】以上説明したように、従来、公開鍵暗号の基本演算である剰余系での乗算と除算を含む演算の繰り返し処理を効率化する算法は実現されておらず、公開鍵暗号の一種である楕円曲線暗号などにおける全体としての処理時間の効率化が困難であるという問題があった。

【００１９】本発明は、上記事情を考慮してなされたもので、モンゴメリ演算域での逆元を高速に求めることのできるモンゴメリ逆元計算装置及び方法、モンゴメリ演算域での除算結果を高速に求めることのできるモンゴメリ除算装置及び方法を提供することを目的とする。

【００２０】

【課題を解決するための手段】本発明（請求項１）は、正の整数Ｎ、正の整数Ａ（０≦Ａ＜Ｎ、ＡとＮは互いに素）、正の整数Ｂについて、Ｎを２進表現したときのビット長をＬとして、ｎ≧Ｌなる整数ｎに対して、$Y=B\cdot A^{-1}\cdot 2^{n} \mod N$なるモンゴメリ演算域での除算結果Ｙを求めるモンゴメリ除算装置であって、整数Ａと法Ｎを入力として逆元$X=A^{-1}\cdot 2^{2n} \mod N$を求めるモンゴメリ逆元計算手段と、求められた逆元Ｘと法ＮとＢを入力として除算結果$Y=B\cdot X\cdot 2^{-n} \mod N$を求めるモンゴメリ乗算手段とを備えたことを特徴とする。

【００２１】本発明（請求項２）は、請求項１に記載のモンゴメリ除算装置において、前記モンゴメリ逆元計算手段は、整数Ａと法Ｎを入力として中間結果$C=A^{-1}\cdot 2^{k} \mod N$とパラメータｋ（Ｌ≦ｋ≦２Ｌ）を求める逆元計算手段と、求められた中間結果Ｃとパラメータｋと法Ｎを入力として逆元$X=C\cdot 2^{2n-k} \mod N$を求める逆元補正手段とを有することを特徴とする。

【００２２】本発明（請求項３）は、正の整数Ｎ、正の整数Ａ（０≦Ａ＜Ｎ、ＡとＮは互いに素）、正の整数Ｂについて、Ｎを２進表現したときのビット長をＬとして、ｎ≧Ｌなる整数ｎに対して、$Y=B\cdot A^{-1}\cdot 2^{n} \mod N$なるモンゴメリ演算域での除算結果Ｙを求めるモンゴメリ除算装置であって、整数Ａと法Ｎを入力として第１の中間結果$C=A^{-1}\cdot 2^{k} \mod N$とパラメータｋ（Ｌ≦ｋ≦２Ｌ）を求める逆元計算手段と、求められた第１の中間結果ＣとＮとＢを入力として第２の中間結果$D=B\cdot C\cdot 2^{-n} \mod N$を求めるモンゴメリ乗算手段と、このモンゴメリ乗算手段により求められた第２の中間結果Ｄと前記逆元計算手段により求められたパラメータｋと法Ｎを入力として除算結果$Y=D\cdot 2^{2n-k} \mod N$を求める逆元補正手段とを備えたことを特徴とする。

【００２３】本発明（請求項４）は、正の奇整数Ｎ、正の整数Ａ（０≦Ａ＜Ｎ、ＡとＮは互いに素）について、Ｎを２進表現したときのビット長をＬとして、ｎ≧Ｌなる整数ｎに対して、$X=A^{-1}\cdot 2^{2n} \mod N$なるモンゴメリ演算域での逆元Ｘを求めるモンゴメリ逆元計算装置であって、整数Ａと法Ｎを入力として中間結果$C=A^{-1}\cdot 2^{k} \mod N$とパラメータｋ（Ｌ≦ｋ≦２Ｌ）を求める逆元計算手段と、求められた中間結果Ｃとパラメータｋと法Ｎを入力として逆元$X=C\cdot 2^{2n-k} \mod N$を求める逆元補正手段とを備えたことを特徴とする。

【００２４】本発明（請求項５）は、請求項４に記載のモンゴメリ逆元計算装置において、内部に中間変数を記憶する複数のレジスタと、前記レジスタを右または左にシフトするビットシフト器と、２つのレジスタの内容の加算または減算を行う加減算器と、２つのレジスタの内容の大小比較およびレジスタ内部の所定のビット位置の値の判定を行う判定器とを用いて前記逆元計算部および前記逆元補正部を構成することを特徴とする。

【００２５】本発明（請求項６）は、正の奇整数Ｎ、正の整数Ａ（０≦Ａ＜Ｎ、ＡとＮは互いに素）について、Ｎを２進表現したときのビット長をＬとして、ｎ≧Ｌなる整数ｎに対して、$X=A^{-1}\cdot 2^{2n} \mod N$なるモンゴメリ演算域での逆元Ｘを求めるモンゴメリ逆元計算装置であって、初期状態を２進表現にてＵ＝Ｎ、Ｖ＝Ａ、Ｔ＝０、Ｓ＝１、ｋ＝０とし、Ｕの最下位ビットが０ならば、Ｕを右シフトし、Ｓを左シフトし、ｋを１増加するとともに、Ｖの最下位ビットが０ならば、Ｖを右シフトし、Ｔを左シフトし、ｋを１増加する処理と、Ｕの最下位ビットが１かつＶの最下位ビットが１で、Ｕ＞Ｖならば、ＵからＶを減じ、Ｕを右シフトし、ＴにＳを加え、Ｓを左シフトし、ｋを１増加する処理と、Ｕの最下位ビットが１かつＶの最下位ビットが１で、Ｕ≦Ｖならば、ＶからＵを減じ、Ｖを右シフトし、ＳにＴを加え、Ｔを左シフトし、ｋを１増加する処理からなる一連のループ処理を、Ｖ＞０の間、繰り返し、Ｖ＝０になった場合、Ｔ≧ＮならばＴからＮを減じた後に、ＮからＴを減じた値をＴとし、Ｔ＜ＮならばＮからＴを減じた値をＴとする逆元計算手段と、初期状態をｉ＝０とし、前記逆元計算手段により求められたＴを左シフトした後、

Ｔ≧ＮならばＴからＮを減じてｉを１増加し、Ｔ＜Ｎならばｉを１増加するループ処理を、ｉ＜２ｎ－ｋの間、繰り返し、ｉ＝２ｎ－ｋになったときのＴを逆元Ｘとする逆元補正手段とを備えたことを特徴とする。

【００２６】本発明（請求項７）は、請求項６に記載のモンゴメリ逆元計算装置において、初期状態としてＮが設定されるＵレジスタと、初期状態としてＡが設定されるＶレジスタと、初期状態として０が設定されるＴレジスタと、初期状態として１が設定されるＳレジスタと、初期状態として０が設定されるｋレジスタと、Ｕレジスタの右シフト、Ｖレジスタの右シフト、Ｔレジスタの左シフト、およびＳレジスタの左シフトのうち指定されたものを実行するビットシフト器と、ＵレジスタからＶレジスタの内容を減じる処理、ＶレジスタからＵレジスタの内容を減じる処理、ＴレジスタにＳレジスタの内容を加える処理、ＳレジスタにＴレジスタの内容を加える処理、ＴレジスタからＮを減じる処理、ＮからＴレジスタの内容を減じる処理、およびｋレジスタに１を加える処理のうち指定されたものを実行する加減算器と、Ｕレジスタの最下位ビットが０であるか否か、Ｖレジスタの最下位ビットが０であるか否か、Ｖレジスタの値が０になったか否か、およびＴレジスタの値がＮ以上であるか否かを判断する判定器と、前記ビットシフト器、前記加減算器および前記判定器を制御する制御部を備えたことを特徴とする。

【００２７】本発明（請求項８）は、正の整数Ｎ、正の整数Ａ（０≦Ａ＜Ｎ、ＡとＮは互いに素）、正の整数Ｂについて、Ｎを２進表現したときのビット長をＬとして、ｎ≧Ｌなる整数ｎに対して、$Y=B\cdot A^{-1}\cdot 2^{n} \mod N$なるモンゴメリ演算域での除算結果Ｙを求めるモンゴメリ除算方法であって、整数Ａと法Ｎを入力として逆元$X=A^{-1}\cdot 2^{2n} \mod N$を求める第１のステップと、求められた逆元Ｘと法ＮとＢを入力として除算結果$Y=B\cdot X\cdot 2^{-n} \mod N$を求める第２のステップとを有することを特徴とする。

【００２８】本発明（請求項９）は、請求項８に記載のモンゴメリ除算方法において、前記第１のステップは、整数Ａと法Ｎを入力として中間結果$C=A^{-1}\cdot 2^{k} \mod N$とパラメータｋ（Ｌ≦ｋ≦２Ｌ）を求め、求められた中間結果Ｃとパラメータｋと法Ｎを入力として逆元$X=C\cdot 2^{2n-k} \mod N$を求めるものであることを特徴とする。

【００２９】本発明（請求項１０）は、正の整数Ｎ、正の整数Ａ（０≦Ａ＜Ｎ、ＡとＮは互いに素）、正の整数Ｂについて、Ｎを２進表現したときのビット長をＬとして、ｎ≧Ｌなる整数ｎに対して、$Y=B\cdot A^{-1}\cdot 2^{n} \mod N$なるモンゴメリ演算域での除算結果Ｙを求めるモンゴメリ除算方法であって、整数Ａと法Ｎを入力として第１の中間結果$C=A^{-1}\cdot 2^{k} \mod N$とパラメータｋ（Ｌ≦ｋ≦２Ｌ）を求める第１のステップと、この第１のステップにより求められた第１の中間結果Ｃと法ＮとＢを入力として第２の中間結果$D=B\cdot C\cdot 2^{-n} \mod N$を求める第２のステップと、この第２のステップにより求められた第２の中間結果Ｄと前記第１のステップにより求められたパラメータｋと法Ｎを入力として除算結果$Y=D\cdot 2^{2n-k} \mod N$を求める第３のステップとを有することを特徴とする。

【００３０】本発明（請求項１１）は、正の奇整数Ｎ、正の整数Ａ（０≦Ａ＜Ｎ、ＡとＮは互いに素）について、Ｎを２進表現したときのビット長をＬとして、ｎ≧Ｌなる整数ｎに対して、$X=A^{-1}\cdot 2^{2n} \mod N$なるモンゴメリ演算域での逆元Ｘを求めるモンゴメリ逆元計算方法であって、整数Ａと法Ｎを入力として中間結果$C=A^{-1}\cdot 2^{k} \mod N$とパラメータｋ（Ｌ≦ｋ≦２Ｌ）を求め、求められた中間結果Ｃとパラメータｋと法Ｎを入力として逆元$X=C\cdot 2^{2n-k} \mod N$を求めることを特徴とする。

【００３１】本発明（請求項１２）は、正の奇整数Ｎ、正の整数Ａ（０≦Ａ＜Ｎ、ＡとＮは互いに素）について、Ｎを２進表現したときのビット長をＬとして、ｎ≧Ｌなる整数ｎに対して、$X=A^{-1}\cdot 2^{2n} \mod N$なるモンゴメリ演算域での逆元Ｘを求めるモンゴメリ逆元計算方法であって、初期状態を２進表現にてＵ＝Ｎ、Ｖ＝Ａ、Ｔ＝０、Ｓ＝１、ｋ＝０とし、Ｕの最下位ビットが０ならば、Ｕを右シフトし、Ｓを左シフトし、ｋを１増加するとともに、Ｖの最下位ビットが０ならば、Ｖを右シフトし、Ｔを左シフトし、ｋを１増加する処理と、Ｕの最下位ビットが１かつＶの最下位ビットが１で、Ｕ＞Ｖならば、ＵからＶを減じ、Ｕを右シフトし、ＴにＳを加え、Ｓを左シフトし、ｋを１増加する処理と、Ｕの最下位ビットが１かつＶの最下位ビットが１で、Ｕ≦Ｖならば、ＶからＵを減じ、Ｖを右シフトし、ＳにＴを加え、Ｔを左シフトし、ｋを１増加する処理からなる一連のループ処理を、Ｖ＞０の間、繰り返し、Ｖ＝０になった場合、Ｔ≧ＮならばＴからＮを減じた後に、ＮからＴを減じた値をＴとし、Ｔ＜ＮならばＮからＴを減じた値をＴとする第１のステップと、初期状態をｉ＝０とし、前記第１のステップにより求められたＴを左シフトした後、Ｔ≧ＮならばＴからＮを減じてｉを１増加し、Ｔ＜Ｎならばｉを１増加するループ処理を、ｉ＜２ｎ－ｋの間、繰り返し、ｉ＝２ｎ－ｋになったときのＴを逆元Ｘとする第２のステップとを有することを特徴とする。

【００３２】本発明によれば、モンゴメリ演算域のままでモンゴメリ逆元計算を行なうモンゴメリ逆元計算手段とモンゴメリ乗算手段を用いるため、モンゴメリ演算域の元を入力として、モンゴメリ演算域での除算結果を直接求めることができる。この結果、モンゴメリ演算域と元の剰余系との変換・逆変換のオーバーヘッドがないため、モンゴメリ演算域での除算が高速に実現できる。

【００３３】また、本発明によれば、モンゴメリ演算域

のままモンゴメリ逆元計算を行なうことができ、モンゴメリ演算域と元の剰余系との変換・逆変換のオーバーヘッドがないため、モンゴメリ演算域での逆元計算が高速に実現できる。

【００３４】また、本発明によれば、モンゴメリ演算域での逆元計算が多倍長レジスタの加減算とビットシフトで実現できるため、ソフトウェア実装・ハードウェア実装のどちらでも高速な装置構成が可能となる。さらに、モンゴメリ演算域での除算も高速な装置構成が実現できる。

【００３５】したがって、楕円曲線暗号などのように剰余系での乗算と除算を含む演算の繰り返し処理を基本演算とする暗号において、全体としての処理時間を高速化することができる。

【００３６】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【００３７】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００３８】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【００３９】なお、以下では、整数ｓ，ｕについてｓ　ｍｏｄ　ｕは、ｓをｕで割ったときの剰余を表すものとする。

【００４０】前述したようにモンゴメリ演算域での乗算は一般に、剰余系での乗算よりも効率良く実装できることが知られており、ＲＳＡ暗号など剰余系の乗算を繰り返す方式を実現する場合、モンゴメリ演算が利用されることがある。しかし、ＲＳＡ暗号のように暗号化・復号化に乗算を用いるだけではなく、除算や逆元計算を用いる暗号もある。例えば、楕円曲線暗号では、剰余系での四則演算を組合せて単位演算が構成され、その単位演算を所定の回数繰り返すことで暗号アルゴリズムが構成される。ところが、モンゴメリ演算域での除算や逆元計算としては効率良く実装できるものがなく、楕円曲線暗号等のように剰余系での四則演算を組合せて単位演算が構成されるものについてはモンゴメリ演算域を利用した処理の効率化が困難であった。

【００４１】本実施形態に係る除算装置、逆元計算装置は、それぞれモンゴメリ演算域での剰余除算、逆元計算の結果を効率的に求めることができるようにしたものである。

【００４２】最初に、通常の剰余系Ｚｐ（ｐを法とする剰余系を表す）とモンゴメリ演算域との関係およびモンゴメリ演算域での演算について説明する。

【００４３】図１２に、モンゴメリ演算域と剰余系Ｚｐの２つの代数系の間における、定義域、元、逆元、および加算、減算、乗算、除算の四則演算の関係を示す。

【００４４】なお、法の値ｐは整数であるが、好ましくは奇整数を用いる。また、暗号システムに適用する場合、ｐには素数を用いることが多い。

【００４５】剰余系Ｚｐでの元をａとするとき、それに対応するモンゴメリ演算域の元Ａには、

$$A = a \cdot R \mod p$$

により与えられる。

【００４６】一方、モンゴメリ演算域の元Ａから剰余系Ｚｐの元ａへの逆変換は、

$$a = A \cdot R^{-1} \mod p$$

により与えられる。

【００４７】ここで、Ｒはモンゴメリ演算域を定義するパラメータであり、その条件は、

（ｉ）Ｒと法ｐとは互いに素であること

（ii）Ｒ＞ｐ

の２つである。

【００４８】一般にＲは２のべき乗（$R = 2^n$）とし、さらにハードウェアのワード長の倍数を用いることが多い。演算幅をできるだけ小さくするためには、法ｐのビット数をＬとした場合に、ｎ≧Ｌを満たし、ワード長の倍数である最小の値を用いることが好ましい。以下では、簡単のために、ｎは法ｐのビット長Ｌと等しいものとして説明する。

【００４９】図１３（ａ）に、ｐ＝２３、$R = 2^5$（ｎ＝５）とした場合の剰余系Ｚｐの元ａとモンゴメリ演算域の元Ａとの対応関係を一例として示す（ただし、現実の暗号装置等で使用するｐは非常に大きな整数である）。

【００５０】モンゴメリ演算域での除算装置や逆元計算装置では、$R = 2^n$ を用いるものとする。

【００５１】次に、モンゴメリ演算域での逆元計算と四則演算は、剰余系Ｚｐの元ａに対し$A = a \cdot R \mod p$なるモンゴメリ演算域の元が対応することを考慮して、図１２のように定義できる。

【００５２】まず、モンゴメリ演算域の加算および減算は、剰余系でのそれらと同様、

$$A + B \mod p$$

$$A - B \mod p$$

で定義される。

【００５３】次に、モンゴメリ乗算は、

$$A \cdot B \cdot R^{-1} \mod p$$

により与えられる。

【００５４】他のモンゴメリ演算域での演算はモンゴメリ乗算$ABR^{-1} \mod p$をもとにすると以下のようのに定義される。

【００５５】Ａの逆元Ｘは、ＡとＸを乗数・被乗数とし

てモンゴメリ乗算を行なったときに、モンゴメリ演算域での単位元となるＲを結果として与えるような値となる。すなわち、逆元Ｘは、

$A \cdot X = R^2 \mod p$

を満たす値である。

【００５６】したがって、モンゴメリ演算域での法をｐとするＡについての逆元計算は、

$X = A^{-1} \cdot R^2 \mod p$

により与えられる。

【００５７】後述する本実施形態に係る逆元計算装置は、入力Ａと法ｐに対して、$X = A^{-1} \cdot R^2 \mod p$を効率的に求める装置である。

【００５８】同様にして、法をｐ、Ａを除数、Ｂを被除数とするモンゴメリ除算は、

$Y = B \cdot A^{-1} \cdot R \mod p$

$= B \cdot A' \cdot R^{-1} \mod p$　（ただし、A'はモンゴメリ演算域でのＡの逆元）

により与えられる。

【００５９】後述する本実施形態に係る除算装置は、入力Ａ，Ｂと法ｐに対して、$B \cdot A' \cdot R \mod p$を効率的に求める装置である。

【００６０】図１３（ｂ）に、ｐ＝２３、Ｒ＝2^5（ｎ＝５）とした場合の剰余系Ｚｐにおける元ａと逆元ｘの対応関係を一例として示す。また、図１３（ｃ）に、ｐ＝２３、Ｒ＝2^5（ｎ＝５）とした場合のモンゴメリ演算域における元Ａと逆元Ｘの対応関係を一例として示す。

【００６１】さて、このようなモンゴメリ演算を利用するには、最初に剰余系Ｚｐからモンゴメリ演算域への変換を行ない、モンゴメリ演算域で所定の演算処理を繰り返した後、モンゴメリ演算域から剰余系Ｚｐへの逆変換を行なう。なお、これら変換・逆変換はそれぞれ多倍長乗算１回程度の処理であり、全体としてはあまり大きなオーバヘッドではない。

【００６２】ここで、モンゴメリ演算を利用した具体例を示す。

【００６３】例えば、ｐ＝２３、Ｒ＝2^5（ｎ＝５）として、モンゴメリ演算を利用し剰余系Ｚｐの元ａ＝３の＊逆元ｘを求める場合を考える。まず、剰余系Ｚｐの元ａ＝３をモンゴメリ演算域の元Ａに変換すると、Ａ＝４が求まる。次に、モンゴメリ演算域の元Ａ＝４の逆元Ｘとして、Ｘ＝３が求まる。そして、モンゴメリ演算域の元Ｘ＝３を剰余系Ｚｐの元ｘに逆変換すると、ｘ＝８が求まる。なお、剰余系Ｚｐの元ａ＝３の逆元ｘを直接、剰余系で求めると、ｘ＝８となり、上記の結果と一致することがわかる。

$$Y = B \cdot (A^{-1} \cdot R^2) \cdot R^{-1} \mod p$$
$$= (B \cdot (A^{-1} \cdot R^2 \mod p) \cdot R^{-1} \mod p$$
$$= B \cdot X \cdot R^{-1} \mod p$$

と変形して、まず、除数Ａと法ｐを入力としてモンゴメリ逆元計算部２０１によりモンゴメリ演算域でのＡの逆元Ｘを求め、次に、このＸと上記の被除数Ｂと法ｐを入力としてモンゴメリ乗算部２０２により$Y = B \cdot X \cdot R^{-1} \mod p$、すなわち$Y = B \cdot A^{-1} \cdot R \mod p$を求める。

【００６４】また、例えば、ｐ＝２３、Ｒ＝2^5（ｎ＝５）として、モンゴメリ演算を利用し剰余系Ｚｐの乗算３×６を行なう場合を考える。まず、剰余系Ｚｐの３と６をモンゴメリ演算域の４と８に変換し、$Y = 4 \times 8 \times R^{-1} \mod p$から、Ｙ＝１が求まる。これを剰余系Ｚｐに逆変換すると、乗算結果としてｙ＝１８が求まる。なお、剰余系Ｚｐで直接$y = 3 \times 6 \mod p$を求めると、ｙ＝１８となり、上記の結果と一致することがわかる。

【００６５】また、例えば、ｐ＝２３、Ｒ＝2^5（ｎ＝５）として、モンゴメリ演算を利用し剰余系Ｚｐの剰余除算６／２を行なう場合を考える。まず、剰余系Ｚｐの６と２をモンゴメリ演算域の８と１８に変換し、被除数１８の逆元として１６を求め、$Y = 8 / 18 \times R^{-1} \mod p = 8 \times 16 \times R^{-1} \mod p$から、Ｙ＝４が求まる。これを剰余系Ｚｐに逆変換すると、除算結果としてｙ＝３が求まる。なお、剰余系Ｚｐで直接$y = 6 / 2 \mod p$を求めると、ｙ＝３となり、上記の結果と一致することがわかる。

【００６６】以下では、本実施形態に係るモンゴメリ演算域での逆元計算装置および除算装置について説明する。

【００６７】図１に、本発明の一実施形態に係るモンゴメリ演算域での除算装置の基本構成を示す。本除算装置２００は、モンゴメリ逆元計算部２０１とモンゴメリ乗算部２０２を備えており、モンゴメリ逆元計算部２０１とモンゴメリ乗算部２０２をシーケンシャルに利用してモンゴメリ除算装置２００を構成している。

【００６８】本実施形態では、モンゴメリ除算$Y = B \cdot A^{-1} \cdot R \mod p$を、

技術を用いることができる。

【００７０】図１４に、モンゴメリ乗算部２０２における処理手順の一例を示す。ここでは、２数Ａ、Ｂに対して、$A \cdot B \cdot R^{-1} \mod N$を求めるものとして表記する。

【００７１】$V = -N^{-1} \mod R$（すなわち、$V \cdot N = -1 \mod R$を満たすＶ）を求め（ステップＳ１０１）、Ｔ＝Ａ・Ｂを求め（ステップＳ１０２）、$W = ((T \mod R) \cdot V) \mod R$を求め（ス

テップＳ１０３）、Ｔ＋Ｗ・ＮをＴに代入し（ステップＳ１０４）、Ｔ＝Ｔ／Ｒを実行する（ステップＳ１０５）。そして、Ｔ＞Ｎならば（ステップＳ１０６）、ＴからＮを減ずる（ステップＳ１０７）。このときに得られるＴが法をＮとするＡとＢのモンゴメリ乗算結果である。なお、Ｒを２のべき乗にとれば、剰余算や除算は２進数の下位の切り出しや上位の切り出しで実現できる。また、Ｖの値を法Ｎについて計算しておくことで、処理の効率化が可能である。

【００７２】図１５に、モンゴメリ乗算部２０２における処理手順の他の例を示す。この処理手順は図１４の処理手順を改良し、必要な演算を多倍長乗算２回程度にしたものである。ここでは、２数Ａ、Ｂに対して、Ａ・Ｂ・R^{-1} ｍｏｄ Ｎを求めるものとして表記する。また、Ａ、Ｂ、Ｎなどは、基数ｂで表現されているものとする。例えば、$A=a_{r-1}b^{r-1}+a_{r-2}b^{r-2}+\cdots+a_1b+a_0$などの形式である。ここで、基数ｂは２のべき乗とし、例えば2^8、2^{16}である。もちろん、ｂ＝２でも構わない。

【００７３】$v_0=-N_0^{-1}$ ｍｏｄ ｂ（すなわち、$v_0\cdot N_0=-1$ ｍｏｄ ｂを満たすv_0）を求め、また、Ｔ＝０、ｉ＝０とし（ステップＳ２０１）、$T+a_iBb^i$をＴに代入し（ステップＳ２０２）、$m_i=t_iv_0$ ｍｏｄ ｂを求め（ステップＳ２０３）、$T+m_iNb^i$をＴに代入し（ステップＳ２０４）、ｉを１増加する。次に、ステップＳ２０６で、ｉ≦（ｒ－１）ならばステップＳ２０２に戻る。また、ステップＳ２０６で、ｉ＞（ｒ－１）ならばループを抜けステップＳ２０７に移り、Ｔ＝Ｔ／Ｒを実行する（ステップＳ２０７）。そして、Ｔ＞Ｎならば（ステップＳ２０８）、ＴからＮを減ずる（ステップＳ２０９）。このときに得られるＴが法をＮとするＡとＢのモンゴメリ乗算結果である。

【００７４】この手順の１つの特徴は、ステップＳ２０７の実行直前において、Ｔの下位側のＬブロックが全て０（すなわち、ＴはＲの倍数）になる点にある。したがって、ワーク領域を削減することが可能となる。また、剰余算は２進数の下位の切り出しで実現できる。また、v_0の値を法Ｎについて計算しておくことで、処理の効率化が可能である。

【００７５】以上のようにモンゴメリ乗算部２０２は、効率的な実現が可能である。また、詳しくは後述するが、本発明によればモンゴメリ逆元計算部２０１を効率的に実現することができる。従って、本実施形態の除算装置２００によれば、モンゴメリ演算域での除算を効率良く実行することができる。

【００７６】図２に、本実施形態に係るモンゴメリ演算域での逆元計算装置２０１の基本構成の一例を示す。もちろん、この逆元計算装置２０１は、図１のモンゴメリ除算装置２００のモンゴメリ逆元計算部２０１として用いることができる。

【００７７】本逆元計算装置２０１は、逆元計算部３０１と逆元補正部３０２を備えており、逆元計算部３０１と逆元補正部３０２をシーケンシャルに利用してモンゴメリ逆元計算装置２０１を構成している。

【００７８】本実施形態では、逆元計算$X=A^{-1}\cdot R^2$ ｍｏｄ ｐ$=A^{-1}\cdot 2^{2n}$ ｍｏｄｐを、

$X=A^{-1}\cdot(2^k\cdot 2^{2n-k})$ ｍｏｄ ｐ

$=(A^{-1}\cdot 2^k)\cdot 2^{2n-k}$ ｍｏｄ ｐ

$=(A^{-1}\cdot 2^k$ ｍｏｄ ｐ$)\cdot 2^{2n-k}$ ｍｏｄ ｐ

$=C\cdot 2^{2n-k}$ ｍｏｄ ｐ

と変形して、まず、整数Ａと法ｐ（ただしＡはｐと互いに素）を入力として逆元計算部３０１により$C=A^{-1}\cdot 2^k$ ｍｏｄ ｐとｋを求める。ここで、ｋはＬ以上２Ｌ以下の整数で、Ａとｐから一意に決定される値である。次に、このＣとｋと法ｐを入力として逆元補正部３０２により逆元$X=C\cdot 2^{2n-k}$ ｍｏｄ ｐ、すなわち$X=A^{-1}\cdot R^2$ ｍｏｄ ｐを求める。

【００７９】図３および図４に、逆元計算部３０１における処理手順の一例を示す。

【００８０】この手順は、Ｕレジスタ、Ｖレジスタ、Ｔレジスタ、Ｓレジスタの４つの多倍長レジスタを利用し、レジスタの左右へのシフト演算とレジスタ同士の加算、減算で構成され、ループの繰り返し回数がループカウンタとして用いる変数ｋに格納される。ｋの値は法ｐのビットサイズをＬとするとき、Ｌ以上２Ｌ以下であり、加減算の処理量はＯ（Ｌ）であるため、全体でも高々Ｏ（L^2）の処理量である。以下、図３および図４の手順を流れを追って説明する。

【００８１】まず、与えられた法ｐをレジスタＵに、ｐ以下の正の整数Ａをレジスタ Ｖに設定する。また、レジスタＴに０、レジスタＳに１、レジスタｋに０をそれぞれ設定する（ステップＳ４０１）。以上が、変数初期化の処理である。

【００８２】以降、ステップＳ４０２からステップＳ４１０の処理を、レジスタＶが正の値である間（０になるまで）、繰り返す。

【００８３】まず、レジスタＶが０でなければ、繰り返し処理を続けるので、ステップＳ４０３にとぶ（ステップＳ４０２）。

【００８４】レジスタＵの最下位ビットが０か否かを判定する（ステップＳ４０３）。もし０であれば、レジスタＵを右に１ビットシフトし（ステップＳ４１１）、レジスタＳを左に１ビットシフトして（ステップＳ４１２）、ステップＳ４１０にとぶ。そして、ステップＳ４１０にてｋの値を１増加し、ステップＳ４０２に戻る。

【００８５】ステップＳ４０３にてレジスタＵの最下位ビットが０でなければ、レジスタＶの最下位ビットが０か否かを判定する（ステップＳ４０４）。もし０であれば、レジスタＶを右に１ビットシフトし（ステップＳ４

１３）、レジスタＴを左に１ビットシフトして（ステップＳ４１４）、ステップＳ４１０にとぶ。そして、ステップＳ４１０にてｋの値を１増加し、ステップＳ４０２に戻る。

【００８６】ステップＳ４０３にてレジスタＵの最下位ビットが０でなく、ステップＳ４０４にてレジスタＶの最下位ビットが０でなければ、レジスタＵとＶの大小比較を行なう（ステップＳ４０５）。

【００８７】もしＵ＞Ｖならば、レジスタＵからレジスタＶの内容を引き（ステップＳ４１５）、レジスタＵを右に１ビットシフトし（ステップＳ４１６）、レジスタＴにレジスタＳの内容を加算し（ステップＳ４１７）、レジスタＳを左に１ビットシフトする（ステップＳ４１８）。そして、ステップＳ４１０にてｋの値を１増加し、ステップＳ４０２に戻る。

【００８８】もしステップＳ４０５の結果、Ｕ＜ＶもしくはＵ＝Ｖの場合は、レジスタＶからレジスタＵの内容を引き（ステップＳ４０６）、レジスタＶを右に１ビットシフトし（ステップＳ４０７）、レジスタＳにレジスタＴの内容を加算し（ステップ４０８）、レジスタＴを左に１ビットシフトする（ステップＳ４０９）。そして、ステップＳ４１０にてｋの値を１増加し、ステップＳ４０２に戻る。

【００８９】以上のループを繰り返し、ステップＳ４０２にてレジスタＶが０になった場合、ステップＳ４１９に移る。そして、まず、レジスタＵの内容が１かどうかをチェックする。レジスタＵの内容は入力Ａと法ｐの最大公約数になるので、もしＵが１でなければＡとｐは互いに素でないことになるので、Ａの逆元は存在しない。そのため、ステップＳ４２３でエラー処理をして終了する。

【００９０】エラーでない場合、すなわちステップＳ４１９にてレジスタＵの内容が１である場合、ステップＳ４２０でＴとｐの大小比較を行ない、もしＴがｐ以上であれば、Ｔからｐを引き（ステップＳ４２１）、Ｔがｐ以下の整数になるようにする。そして、ステップＳ４２２でｐからＴの内容を引いた結果をＴに格納して処理を終了する。

【００９１】以上の処理により、Ｔの内容には$A^{-1}\cdot 2^{k} \mod p$の計算結果が格納される。

【００９２】次に、この$T=A^{-1}\cdot 2^{k} \mod p$とｋの値を逆元補正部３０２に入力して、モンゴメリ逆元値を計算する。

【００９３】図５に、逆元補正部３０２の処理手順の一例を示す。以下、図５の手順を流れを追って説明する。

【００９４】まず、$R=2^{n}$であるところのｎを２倍した値をＬにし、ループカウンタｉを０に設定する（ステップＳ５０１）。

【００９５】次に、ループの繰り返し回数としてＬ－ｋの値を求め、ｍに設定する（ステップＳ５０２）。

【００９６】以降、ステップＳ５０３からステップＳ５０７の処理を、ループカウンタがｍになるまで繰り返す。

【００９７】すなわち、ステップＳ５０３でｉとｍを比較し、ｉがｍ未満の場合には、まず、レジスタＴを１ビット左シフトする（ステップＳ５０４）。次に、Ｔとｐの大小比較を行ない（ステップＳ５０５）、もしＴがｐ以上であればＴからｐを引く（ステップＳ５０６）。そして、ステップＳ５０７にてｉの値を１増加し、ステップＳ５０３に戻る。

【００９８】ステップＳ５０３でｉ＝ｍの場合には、上記の処理ループを抜ける。このループを抜けた時点でのＴの値がモンゴメリ逆元値である。最後に、ステップＳ５０８で逆元の値Ｔを出力して処理を終了する。

【００９９】以上に示した図３、図４、図５の手順はレジスタの加減算とビットシフトのみで実現されるため、効率的な装置化が可能である。

【０１００】以下では、具体例を用いて、本実施形態のモンゴメリ逆元計算装置（または除算装置２００のモンゴメリ逆元計算部）２０１の動作を説明する。

【０１０１】ここでは、一例として、法の値ｐ＝２３、$R=2^{5}$（ｎ＝５）としたときに、モンゴメリ演算域での元Ａ＝１９の逆元を求める場合について示す。

【０１０２】図６（ａ）、（ｂ）には、逆元計算部３０１における、Ｕレジスタ、Ｖレジスタ、Ｔレジスタ、Ｓレジスタのそれぞれの内容を２進数で表した値（ただし、ＴレジスタとＳレジスタにおける上位側ビットの０の表示は省略してある）と、ループカウンタｋの内容を１０進数で表した値の変遷を、各処理ループについて示す。

【０１０３】また、図６（ｃ）には、逆元補正部３０２における、Ｔレジスタの内容を２進数で表した値（ただし、上位側ビットの０の表示は省略してある）の変遷を、各処理ループについて示す。

【０１０４】まず、逆元計算部３０１において、初期化処理の結果、Ｕレジスタ＝ｐ＝１０１１１、Ｖレジスタ＝Ａ＝１００１１、Ｔレジスタ＝０、Ｓレジスタ＝１、ｋ＝０が設定される。

【０１０５】１回目のループでは、Ｕ＞ＶからステップＳ４０５にてＹｅｓとなり、ステップＳ４１５～Ｓ４１８とＳ４１０が実行される。この結果、Ｕレジスタ＝０００１０、Ｖレジスタ＝１００１１、Ｔレジスタ＝１、Ｓレジスタ＝１０、ｋ＝１となる。

【０１０６】２回目のループでは、ＬＳＢ（Ｕ）＝０からステップＳ４０３にてＹｅｓとなり、ステップＳ４１１とＳ４１２とＳ４１０が実行される。この結果、Ｕレジスタ＝００００１、Ｖレジスタ＝１００１１、Ｔレジスタ＝１０、Ｓレジスタ＝１００、ｋ＝２となる。

【０１０７】３回目のループでは、Ｕ＜ＶからステップＳ４０５にてＮｏとなり、ステップＳ４０６～Ｓ４０９

とＳ４１０が実行される。この結果、Ｕレジスタ＝００００１、Ｖレジスタ＝０１００１、Ｔレジスタ＝１０、Ｓレジスタ＝１０１、ｋ＝３となる。

【０１０８】以上のようにして処理を繰り返した結果、７回目のループの実行後、Ｕレジスタ＝００００１、Ｖレジスタ＝００００、Ｔレジスタ＝１００００、Ｓレジスタ＝１０１１１、ｋ＝７となり、Ｖレジスタ＝００００となったので、処理ループを抜ける。

【０１０９】次に、Ｕ＝１であるからステップＳ４１９にてｙｅｓとなり、Ｔ＞ｐであるからステップＳ４２０にＹｅｓとなり、この結果、ステップＳ４２１にてＴ＝Ｔ－Ｐ＝１００００－１０１１１＝１００１となり、最後にステップＳ４２２にてＴ＝ｐ－Ｔ＝１０１１１－１００１＝１１１０となる。

【０１１０】従って、逆元計算部３０１の出力は、Ｔ＝１１１０（＝１０進数表現で１４）、ｋ＝７となる。

【０１１１】次に、逆元補正部３０２において、初期状態として、Ｔ＝１１１０、ｉ＝０、ｍ＝３に設定される（ｉとｍの値は１０進数で表す）。

【０１１２】１回目のループでは、Ｔレジスタが左シフトされてＴ＝１１１００となり、ステップＳ５０５でＹｅｓとなるためステップＳ５０６にてＴ＝１０１となり、そしてｉ＝１となる。

【０１１３】２回目のループでは、Ｔレジスタが左シフトされてＴ＝１０１０となり、ステップＳ５０５でＮｏとなるためステップＳ５０６は実行されず、ｉ＝２となる。

【０１１４】３回目のループでは、Ｔレジスタが左シフトされてＴ＝１０１００となり、ステップＳ５０５でＮｏとなるためステップＳ５０６は実行されず、ｉ＝３＝ｍとなり、処理ループを抜ける。

【０１１５】この結果、出力Ｔ＝１０１００＝１０進数表現で２０となる。

【０１１６】このようにして、法の値ｐ＝２３、Ｒ＝2^5（ｎ＝５）としたときにおける、モンゴメリ演算域での元Ａ＝１９の逆元Ｘ＝２０を得ることができる。

【０１１７】なお、モンゴメリ演算域での元１９と２０にそれぞれ対応する、剰余系Ｚｐでも元を求めると、２０と１５になる。すなわち、剰余系Ｚｐでの元２０の逆元として、１５が得られたことになる。

【０１１８】以下では、前述した逆元計算部３０１や逆元補正部３０２における処理の他の例をそれぞれ示す。

【０１１９】まず、図７および図８に逆元計算部３０１の処理手順の他の例を示す。この手順は図３および図４に示した処理手順と原理的には同じであるが、図３および図４の手順においてステップＳ４０３とステップＳ４０４でそれぞれ多倍長レジスタＵとＶの最下位ビットだけを判定の基準に用い、最下位ビットが０の場合に後続の手順であるステップＳ４１１およびステップＳ４１２、ステップＳ４１３およびステップＳ４１４で１ビットだけレジスタのシフトを行っていたものを、最下位ビットから０が複数連続する場合には一度に複数ビットのシフトを可能とするように改良したものである。このように、一度に複数ビットをまとめて処理する方が有利な場合は多く、特にソフトウェア実装において高速となる。

【０１２０】以下、図７および図８の手順を流れを追って説明する。

【０１２１】まず、入力として与えられた法ｐをレジスタＵに、ｐ以下の正の整数Ａをレジスタ Ｖに設定する。また、レジスタＴに０、レジスタＳに１、レジスタｋに０をそれぞれ設定する（ステップＳ６０１）。

【０１２２】以降、ステップＳ６０２からステップＳ６１２の処理を、レジスタＶが正の値である間（０になるまで）、繰り返す。

【０１２３】ステップＳ６０２でレジスタＶが０でなければ、まず、レジスタＵの最下位ビットからの“０”の連長をカウントしてこの値をｗとする（ステップＳ６０３）。次にｗが０か否かを判定し（ステップＳ６０４）、もし０でなければ、レジスタＵをｗビットだけ右シフトし（ステップＳ６１３）、レジスタＳをｗビットだけ左シフトし（ステップＳ６１４）、ループカウンタＫにｗを加え（ステップＳ６１５）、ステップＳ６０２へとぶ。

【０１２４】ステップＳ６０４でｗが０ならば、レジスタＶの最下位ビットからの“０”の連長をカウントしてこの値をｗとする（ステップ６０５）。次にｗが０かどうかを判定し（ステップＳ６０６）、もし０でなければ、レジスタＶをｗビットだけ右シフトし（ステップＳ６１６）、レジスタＴをｗビットだけ左シフトし（ステップＳ６１７）、ループカウンタＫにｗを加え（ステップＳ６１８）、ステップＳ６０２へとぶ。

【０１２５】ステップＳ６０６でｗが０ならば、レジスタＵとＶの大小比較をし（ステップＳ６０７）、もしＵ＞Ｖならば、レジスタＵからレジスタＶの内容を引き（ステップＳ６１９）、レジスタＵを右に１ビットシフトし（ステップＳ６２０）、レジスタＴにレジスタＳの内容を加算し（ステップＳ６２１）、レジスタＳを左に１ビットシフトし（ステップＳ６２２）、ループカウンタＫに１を加え（ステップＳ６２３）、ステップＳ６０２へとぶ。

【０１２６】もしステップＳ６０７の結果、Ｕ＜ＶもしくはＵ＝Ｖの場合は、レジスタＶからレジスタＵの内容を引き（ステップＳ６０８）、レジスタＶを右に１ビットシフトし（ステップＳ６０９）、レジスタＳにレジスタＴの内容を加算し（ステップＳ６１０）、レジスタＴを左に１ビットシフトし（ステップＳ８１１）、ループカウンタＫに１を加え（ステップＳ６２３）、ステップＳ６０２へもどる。

【０１２７】以上のループを繰り返し、ステップＳ６０

２でレジスタＶが０になった場合、処理ループを抜け、まず、レジスタＵの内容が１かどうかをチェックする（ステップＳ６２４）。レジスタＵの内容は入力Ａと法ｐの最大公約数になるので、もしＵが１でなければステップＳ６２８でエラー処理をして終了する。

【０１２８】エラーでない場合、すなわちステップＳ６２４にてレジスタＵの内容が１である場合、レジスタＴとｐの大小比較をし（ステップＳ６２５）、もしＴがｐ以上であれば、Ｔからｐを引き（ステップＳ６２６）、Ｔがｐ以下の整数になるようにする。そして、ステップＳ６２７でｐからＴの内容を引いた結果をＴに格納して処理を終了する。

【０１２９】以上の処理により、Ｔの内容として$A^{-1}\cdot 2^{k} \mod p$が計算される。

【０１３０】次に、逆元補正部３０２の処理の流れの別の一例を図９、図１０に示す。

【０１３１】この手順も図５に示した処理手順と原理的には同じであるが、図５の手順においてステップＳ５０４で多倍長レジスタＴを１ビットだけ左シフトを行うことを繰り返していたものを、一度に複数ビットのシフトを可能とするように改良したものである。このように、一度に複数ビットをまとめて処理する方が有利な場合は多く、特にソフトウェア実装において高速となる。

【０１３２】以下、図９、図１０の手順を流れを追って説明する。

【０１３３】まず、$R=2^{n}$であるところのｎを２倍した値をＬにし、ループカウンタｉを０に設定する（ステップＳ７０１）。

【０１３４】次に、ループの繰り返し回数としてＬ－ｋの値を求め、ｍに設定する（ステップＳ７０２）。

【０１３５】以降、ステップＳ７０３からステップＳ７１０の処理を、ループカウンタｉがｍになるまで繰り返す。

【０１３６】ステップＳ７０３でｉとｍを比較し、ｉがｍ未満の場合には、まず、レジスタＴを法ｐと同じサイズの２進数と見たときに最上位ビットからの“０”の連長をカウントしてこの値をｗとする（ステップＳ７０４）。

【０１３７】次に、ｗが０かどうかを判定し（ステップＳ７０５）、もし０ならばレジスタＴを１ビットだけ左シフトする（ステップＳ７１２）。この結果、Ｔの値はｐより大きくなるのでステップＳ７１３でレジスタＴからｐの値を減ずる。そして、ループカウンタｉに１を加え（ステップＳ７１４）、ステップＳ７０３へとぶ。ステップＳ７０５でｗが０でなければ、次にｉ＋ｗを計算＊し、この値とｍの大小比較を行う（ステップＳ７０６）。もしｉ＋ｗ＞ｍならば、ｗをｍ－ｉとし（ステップＳ７１５）、レジスタＴをｗビットだけ左シフトする（ステップＳ７１６）。ループカウンタはｍとする（ステップＳ７１７）。ここではステップＳ７１６の左シフトの結果は必ずｐよりも小さいため、補正は不要であり、ステップＳ７０３へとぶ。

【０１３８】ステップＳ７０６でｉ＋ｗ＜ｍもしくはｉ＋ｗ＝ｍの場合には、レジスタＴをｗビットだけ左シフトする（ステップＳ７０７）。この結果、Ｔの値はｐより大きくなる可能性があるので、ステップＳ７０８でＴとｐの大小比較を行い、Ｔがｐ以上の場合はＴからｐの値を減ずる（ステップＳ７０９）。最後にループカウンタｉにｗを加え（ステップＳ７１０）、ステップＳ７０３に戻る。

【０１３９】以上のループを繰り返し、ステップＳ７０３でｉ＝ｍになった場合、処理ループを抜ける。このループを抜けた時点でのＴの値がモンゴメリ逆元値であり、この値を出力して（ステップＳ７１１）、処理を終了する。

【０１４０】以上に示した図７と図８、図９と図１０の手順もレジスタの加減算とビットシフトのみで実現される。

【０１４１】なお、図２のモンゴメリ逆元計算装置や図１のモンゴメリ除算装置のモンゴメリ逆元計算部において、逆元計算部３０１としては、図３と図４、図７および図８のいずれかを、また、逆元補正部３０２としては、図５、図９と図１０のいずれかを、それぞれ任意に組み合わせて利用可能である。

【０１４２】ところで、本モンゴメリ除算装置は、図１で例示した構成に限定されず、他の構成も可能である。図１６に、本実施形態に係るモンゴメリ除算装置の基本構成の他の例を示す。

【０１４３】図２に例示したようにモンゴメリ逆元計算機装置は、一例として、逆元計算部３０１と逆元補正部３０２に分割できるが、図１６では、この逆元計算部３０１をモンゴメリ乗算部２０２の前段に、また、逆元補正部３０２をモンゴメリ乗算部２０２の後段に配置した構成となっている。これは、逆元計算部３０１の出力Ｃに対しては、逆元補正部３０２の演算も、モンゴメリ乗算部２０２の演算も共に乗算であることから、その順序に対する可換性が成立することに基づいている。これを数式で表現すると以下のようになる。

【０１４４】

$$
\begin{aligned}
Y &= B\cdot A^{-1}\cdot R \mod p \\
&= B\cdot (A^{-1}2^{k})\,2^{-k}\cdot (R^{-1}R^{2}) \mod p \\
&= B\cdot (A^{-1}2^{k} \mod p)\cdot R^{-1}(R^{2}\cdot 2^{-k}) \mod p \\
&= (B\cdot C\cdot R^{-1} \mod p)\cdot 2^{2n-k} \mod p \\
&= D\cdot 2^{2n-k} \mod p
\end{aligned}
$$

このようにモンゴメリ除算装置は必ずしもモンゴメリ逆元計算部とモンゴメリ乗算部をシーケンシャルに利用しなくても構成できる。重要なことは、モンゴメリ除算であるＹ＝Ｂ（Ａ$^{-1}$）Ｒ　ｍｏｄ　ｐを効率的に計算することであり、そのためにモンゴメリ逆元計算装置の構成部品（モジュール）である逆元計算部と逆元補正部を分離して用いることもできる。

【０１４５】以上のように本実施形態によれば、楕円曲線暗号など多倍長の四則演算の繰り返し処理を高速に処理する場合に、モンゴメリ演算域での元を入力として、モンゴメリ逆元計算やモンゴメリ除算を実行することができる。したがって、最初に元の剰余系からモンゴメリ演算域に元を変換した後は、モンゴメリ演算域のままで繰り返し処理を実行できる。最後にモンゴメリ演算域から元の剰余系に逆変換すれば良いので全体としてのモンゴメリ変換・逆変換のオーバーヘッドを小さくできる。また、本実施形態のモンゴメリ逆元計算およびモンゴメリ除算は多倍長レジスタの加減算とビットシフトのみで実現できるため、ソフトウェア・ハードウェアのどちらでも効率良く実現できる。

【０１４６】以下では、本実施形態に係るモンゴメリ演算域での逆元計算装置のハードウェア構成について説明する。

【０１４７】図１１に、本逆元計算装置の一構成例をブロック図で示す。

【０１４８】本逆元計算装置は、多倍長レジスタＵ（８０１）、多倍長レジスタＶ（８０２）、多倍長レジスタＳ（８０３）、多倍長レジスタＴ（８０４）とループカウンタとなる単精度のレジスタＫ（８０５）、演算部として加減算器８０６とビットシフタ８０７、加減算器８０６の出力を格納する多倍長のレジスタ８０８とビットシフタ８０７の出力を格納する多倍長のレジスタ８０９、そして全体の動作を制御する制御部（図示せず）を構成要素として持つ。これらの各構成要素は、データ・バス８１０に結線されており、相互にデータの転送が可能である。制御部では、前述したような処理手順に従いレジスタの特定ビットの０／１判定やレジスタの特定部分の０の連長の検査なども行う。

【０１４９】図２における逆元計算部３０１は、この構成要素を図３および図４、もしくは図７および図８に従う動作を行うように制御することによって実現され、図２における逆元補正部３０２は、法ｐを空いているレジスタ（例えばＵレジスタ）に設定し、図５もしくは図９および図１０に従う動作を行うように制御することによって実現される。

【０１５０】なお、以上の各機能は、ソフトウェアとしても実現可能である。

【０１５１】また、本実施形態は、コンピュータに所定の手順を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体として実施することもできる。

【０１５２】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０１５３】

【発明の効果】本発明によれば、モンゴメリ演算域での逆元計算と乗算を行って除算結果を得るので、モンゴメリ演算域の元を入力として、モンゴメリ演算域での除算結果を直接求めることができる。この結果、モンゴメリ演算域と元の剰余系との変換・逆変換のオーバーヘッドがないため、モンゴメリ演算域での除算が高速に実現できる。

【０１５４】また、本発明によれば、モンゴメリ演算域のままモンゴメリ逆元計算を行なうことができ、モンゴメリ演算域と元の剰余系との変換・逆変換のオーバーヘッドがないため、モンゴメリ演算域での逆元計算が高速に実現できる。

【０１５５】また、本発明によれば、モンゴメリ演算域での逆元計算が多倍長レジスタの加減算とビットシフトで実現できるため、ソフトウェア実装・ハードウェア実装のどちらでも高速な装置構成が可能となる。さらに、モンゴメリ演算域での除算も高速な装置構成が実現できる。

【０１５６】したがって、楕円曲線暗号などのように剰余系での乗算と除算を含む演算の繰り返し処理を基本演算とする暗号において、全体としての処理時間を高速化することができる。

【図面の簡単な説明】

【図１】本発明に係るモンゴメリ演算域での除算計算装置の一構成例を示す図

【図２】本発明に係るモンゴメリ演算域での逆元計算装置の一構成例を示す図

【図３】図２の逆元計算部での処理手順の一例を示すフローチャート

【図４】図２の逆元計算部での処理手順の一例を示すフローチャート

【図５】図２の逆元補正部での処理手順の一例を示すフローチャート

【図６】図２の逆元計算装置の具体的な動作例を説明するための図

【図７】図２の逆元計算部での処理手順の他の例を示すフローチャート

【図８】図２の逆元計算部での処理手順の他の例を示すフローチャート

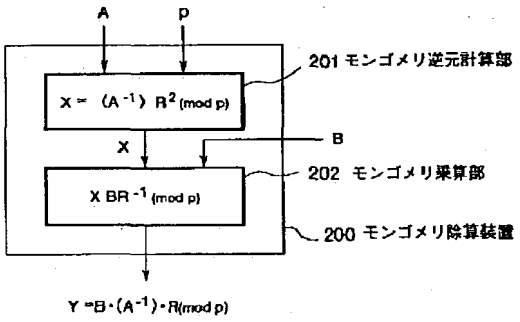
【図９】図２の逆元補正部での処理手順の他の例を示すフローチャート

【図１０】図２の逆元補正部での処理手順の他の例を示すフローチャート

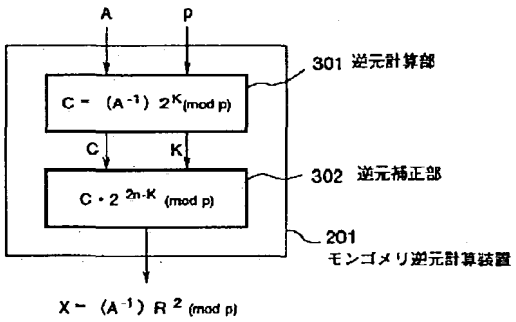
【図１１】本発明に係るモンゴメリ演算域での逆元計算装置のハードウェア構成を示すブロック図
【図１２】モンゴメリ演算域と剰余系Ｚｐの演算の対応を示す図
【図１３】モンゴメリ演算域と剰余系Ｚｐの元および逆元の具体例を示す図
【図１４】図１のモンゴメリ乗算部での処理の一例を示すフローチャート
【図１５】図１のモンゴメリ乗算部での処理の他の例を示すフローチャート
【図１６】本発明に係るモンゴメリ演算域での除算計算装置の他の構成例を示す図

＊【符号の説明】
２００…モンゴメリ除算装置
２０１…モンゴメリ逆元計算装置（モンゴメリ逆元計算部）
２０２…モンゴメリ乗算部
３０１…逆元計算部
３０２…逆元補正部
８０１，８０２，８０３，８０４，８０５，８０８，８０９…レジスタ
８０６…加減算器
８０７…ビットシフタ

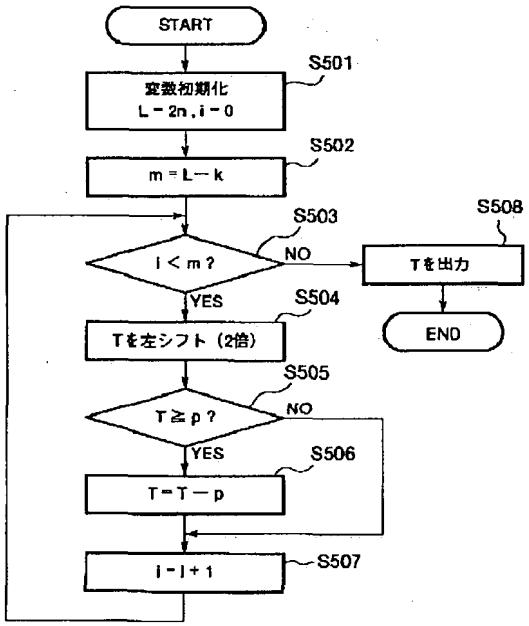
【図１】



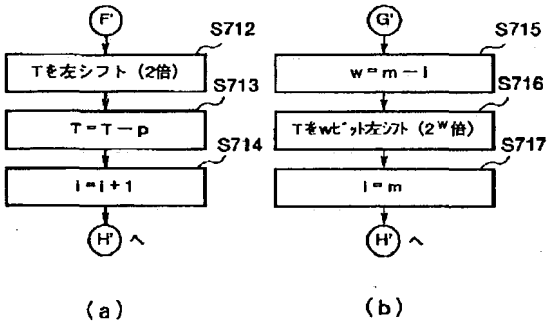
【図２】



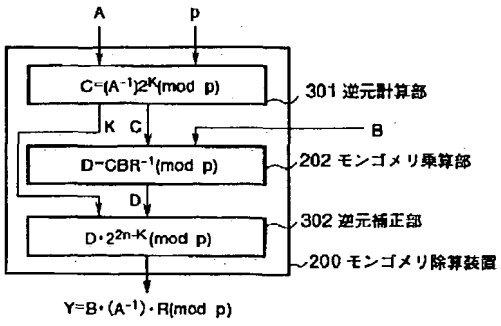
【図５】



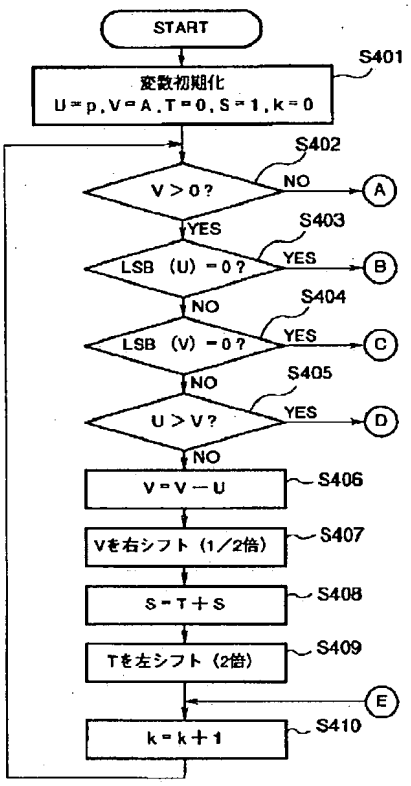
【図１０】



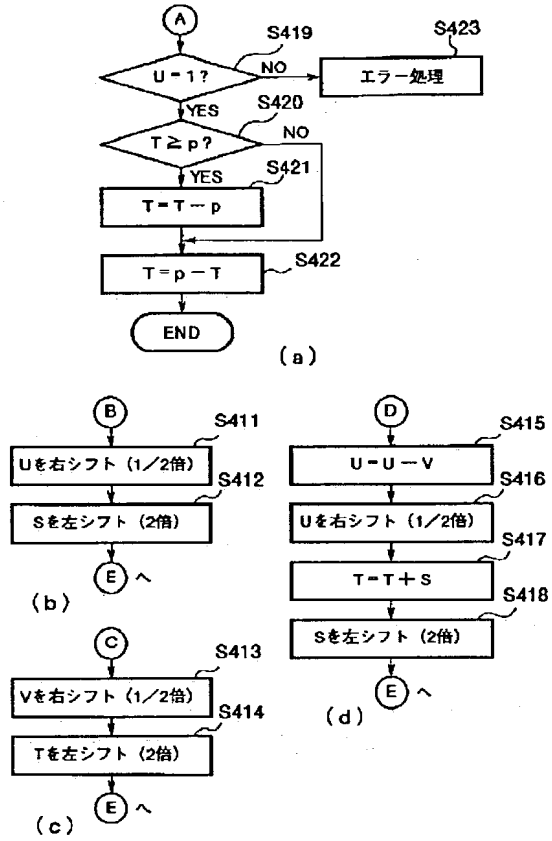
【図１６】



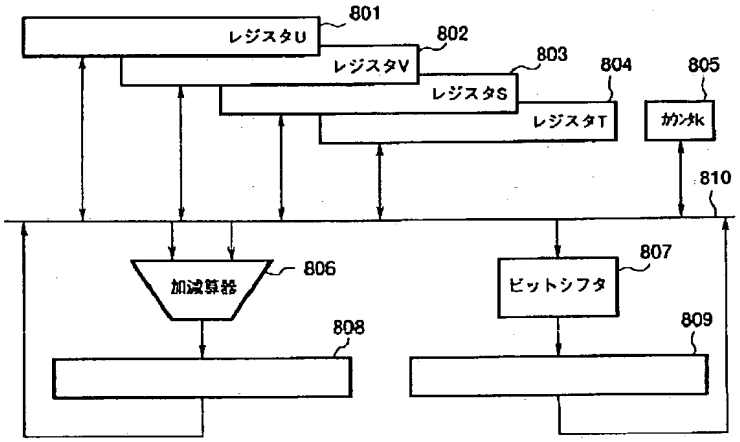
【図３】


START
変数初期化
U＝p，V＝A，T＝0，S＝1，k＝0
S401
V＞0？
S402
NO
A
YES
LSB (U) ＝0？
S403
YES
B
NO
LSB (V) ＝0？
S404
YES
C
NO
U＞V？
S405
YES
D
NO
V＝V－U
S406
Vを右シフト（1／2倍）
S407
S＝T＋S
S408
Tを左シフト（2倍）
S409
E
k＝k＋1
S410

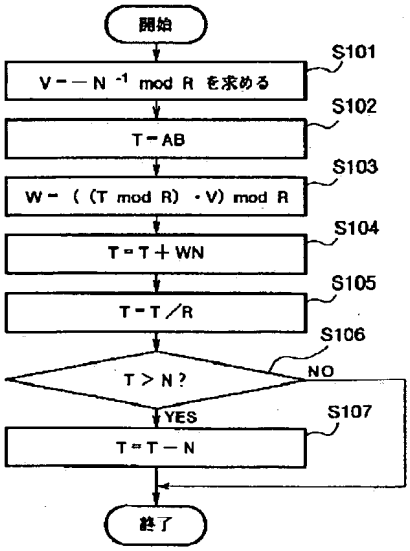
【図４】


A
U＝1？
S419
NO
S423
エラー処理
YES
T≧p？
S420
NO
YES
T＝T－p
S421
T＝p－T
S422
END
(a)
B
Uを右シフト（1／2倍）
S411
Sを左シフト（2倍）
S412
E へ
(b)
C
Vを右シフト（1／2倍）
S413
Tを左シフト（2倍）
S414
E へ
(c)
D
U＝U－V
S415
Uを右シフト（1／2倍）
S416
T＝T＋S
S417
Sを左シフト（2倍）
S418
E へ
(d)

【図１１】


レジスタU
801
レジスタV
802
レジスタS
803
レジスタT
804
カウンタk
805
810
加減算器
806
ビットシフタ
807
808
809

【図１４】


開始
V＝－N -1 mod R を求める
S101
T＝AB
S102
W＝（(T mod R)・V) mod R
S103
T＝T＋WN
S104
T＝T／R
S105
T＞N？
S106
NO
YES
T＝T－N
S107
終了

【図６】

(a)

	初期値	1回目	2回目	3回目	4回目
U (=p)	10111	00010	00001	00001	00001
V (=A)	10011	10011	10011	01001	00100
T	0	1	1	10	100
S	1	10	100	101	111
k	0	1	2	3	4

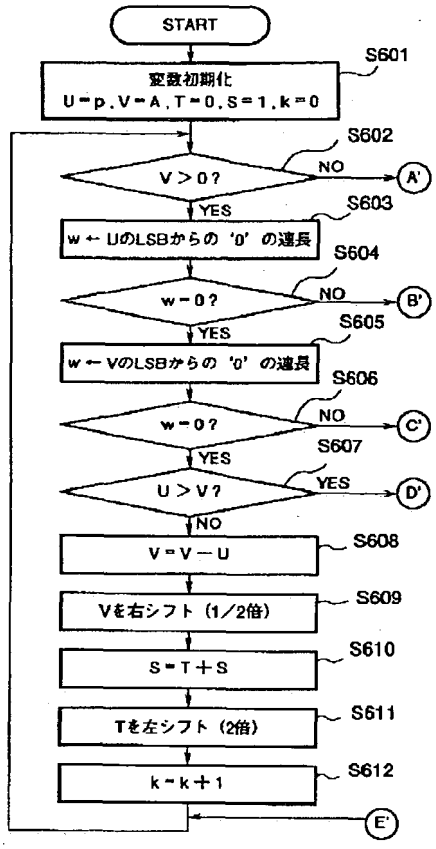
(b)

	5回目	6回目	7回目	出力値
U (=p)	00001	00001	00001	
V (=A)	00010	00001	00000	
T	1000	10000	100000	1110
S	111	111	10111	
k	5	6	7	7

(c)

	T
初期値	1110
1回目 左シフト	11100
pを減算	101
2回目 左シフト	1010
3回目 左シフト	10100

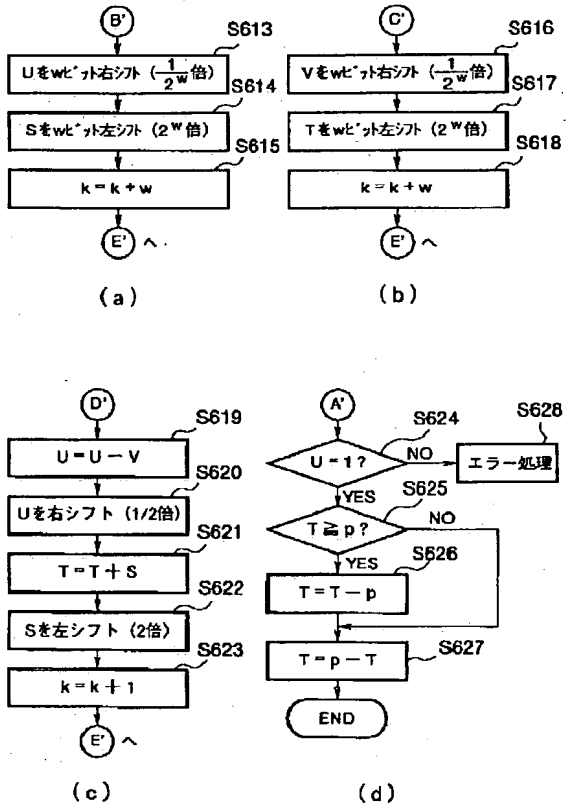
【図７】



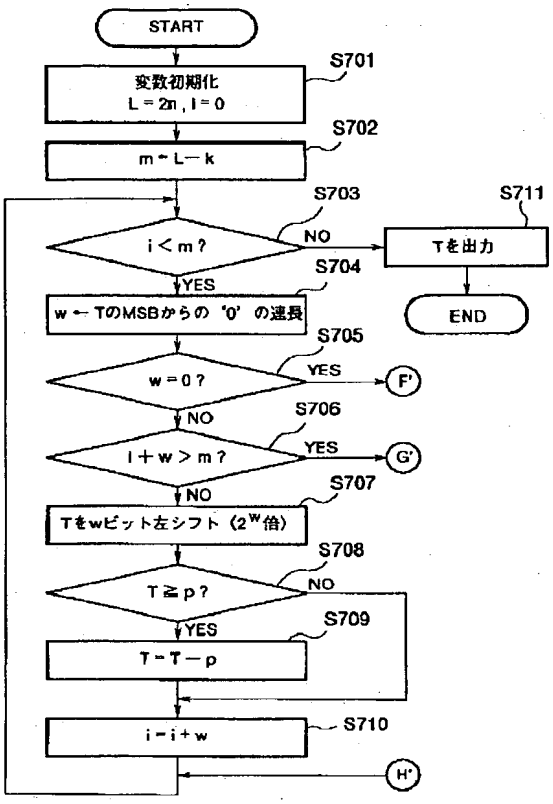
【図１２】

	剰余系Zp領域	モンゴメリ演算域
定義域	0以上 (p−1) 以下の整数	0以上 (p−1) 以下の整数
元	$a=AR^{-1} \bmod p$	$A=aR \bmod p$
逆元	$ax=1 \bmod p$ を満たすx	$Ax=R^2 \bmod p$ を満たすx
加算	$a+b \bmod p$	$A+B \bmod p$
減算	$a-b \bmod p$	$A-B \bmod p$
乗算	$ab \bmod p$	$ABR^{-1} \bmod p$
除算	$b/a=ba^{-1} \bmod p$ (ただし、a^{-1} はaの逆元)	$B/A=BA^{-1}R^{-1} \bmod p$ (ただし、A^{-1} はAの逆元)

【図８】



【図９】



【図１３】

$A = a2^n \bmod p$ $p = 23$ $(n = 5)$

a	A
0	0
1	9
2	18
3	4
4	13
5	22
6	8
7	17
8	3
9	12
10	21
11	7
12	16
13	2
14	11
15	20
16	6
17	15
18	1
19	10
20	19
21	5
22	14

(a)

$ax = 1 \bmod p$ $p = 23$ $(n = 5)$

a	x
1	1
2	12
3	8
4	6
5	14
6	4
7	10
8	3
9	18
10	7
11	21
12	2
13	16
14	5
15	20
16	13
17	19
18	9
19	17
20	15
21	11
22	22

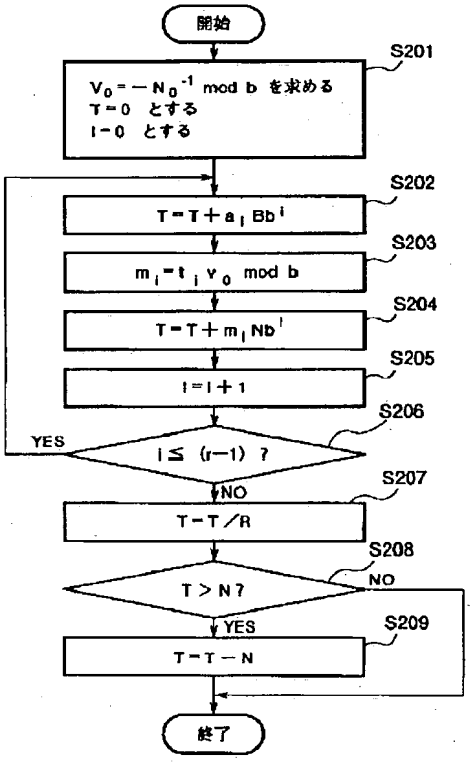
(b)

$AX = 2^{2n} \bmod p$ $p = 23$ $(n = 5)$

A	X
1	12
2	6
3	4
4	3
5	7
6	2
7	5
8	13
9	9
10	15
11	22
12	1
13	8
14	14
15	10
16	18
17	21
18	16
19	20
20	19
21	17
22	11

(c)

【図１５】


開始
S201
$V_0 = -N_0^{-1} \bmod b$ を求める
T=0 とする
I=0 とする
S202
$T = T + a_I Bb^I$
S203
$m_I = t_I v_0 \bmod b$
S204
$T = T + m_I Nb^I$
S205
I=I+1
S206
YES
$I \leq (r-1)$?
NO
S207
T=T/R
S208
T > N ?
NO
YES
S209
T=T−N
終了

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成１１年（１９９９）１１月５日

【公開番号】特開平１０－２６９０６０
【公開日】平成１０年（１９９８）１０月９日
【年通号数】公開特許公報１０－２６９１
【出願番号】特願平１０－１４２５０
【国際特許分類第６版】
G06F 7/72
G09C 1/00 650
// G06F 17/10
【ＦＩ】
G06F 7/72
G09C 1/00 650 A
G06F 15/31 Z

【手続補正書】
【提出日】平成１０年１２月１７日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項６
【補正方法】変更
【補正内容】
【請求項６】正の奇整数N、正の整数A（０≦A＜N、AとNは互いに素）について、Nを２進表現したときのビット長をLとして、n≧Lなる整数nに対して、X＝$A^{-1}\cdot 2^{2n} \bmod N$なるモンゴメリ演算域での逆元Xを求めるモンゴメリ逆元計算装置であって、
初期状態を２進表現にてU＝N、V＝A、T＝０、S＝１、k＝０とし、
Uの最下位ビットが０ならば、Uを右シフトし、Sを左シフトし、kを１増加する処理と、
Vの最下位ビットが０ならば、Vを右シフトし、Tを左シフトし、kを１増加する処理と、
Uの最下位ビットが１かつVの最下位ビットが１で、U＞Vならば、UからVを減じ、Uを右シフトし、TにSを加え、Sを左シフトし、kを１増加する処理と、
Uの最下位ビットが１かつVの最下位ビットが１で、U≦Vならば、VからUを減じ、Vを右シフトし、SにTを加え、Tを左シフトし、kを１増加する処理からなる一連のループ処理を、V＞０の間、繰り返し、
V＝０になった場合、T≧NならばTからNを減じた後に、NからTを減じた値をTとし、T＜NならばNからTを減じた値をTとする逆元計算手段と、
初期状態をｉ＝０とし、
前記逆元計算手段により求められたTを左シフトした後、T≧NならばTからNを減じてｉを１増加し、T＜Nならばｉを１増加するループ処理を、ｉ＜２ｎ－ｋの間、繰り返し、
ｉ＝２ｎ－ｋになったときのTを逆元Xとする逆元補正手段とを備えたことを特徴とするモンゴメリ逆元計算装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２５
【補正方法】変更
【補正内容】
【００２５】本発明（請求項６）は、正の奇整数N、正の整数A（０≦A＜N、AとNは互いに素）について、Nを２進表現したときのビット長をLとして、n≧Lなる整数nに対して、X＝X＝$A^{-1}\cdot 2^{2n} \bmod N$なるモンゴメリ演算域での逆元Xを求めるモンゴメリ逆元計算装置であって、初期状態を２進表現にてU＝N、V＝A、T＝０、S＝１、k＝０とし、Uの最下位ビットが０ならば、Uを右シフトし、Sを左シフトし、kを１増加する処理と、Vの最下位ビットが０ならば、Vを右シフトし、Tを左シフトし、kを１増加する処理と、Uの最下位ビットが１かつVの最下位ビットが１で、U＞Vならば、UからVを減じ、Uを右シフトし、TにSを加え、Sを左シフトし、kを１増加する処理と、Uの最下位ビットが１かつVの最下位ビットが１で、U≦Vならば、VからUを減じ、Vを右シフトし、SにTを加え、Tを左シフトし、kを１増加する処理からなる一連のループ処理を、V＞０の間、繰り返し、V＝０になった場合、T≧NならばTからNを減じた後に、NからTを減じた値をTとし、T＜NならばNからTを減じた値をTとする逆元計算手段と、初期状態をｉ＝０とし、前記逆元計算手段により求められたTを左シフトした後、T≧NならばTからNを減じてｉを１増加し、T＜Nならばｉを１増加するループ処理を、ｉ＜２ｎ－ｋの間、繰り返し、ｉ＝２ｎ－ｋになったときのTを逆元Xとす

る逆元補正手段とを備えたことを特徴とする。